IN. Ref.
6/4/03
6/12

WEST Search History

9/182279

DATE: Wednesday, June 04, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L10	l9 and (manufactur$ with tag$)	2	L10
L9	5768384.pn. or 5673318.pn.	2	L9
L8	l2 and (manufactur$ with tag$)	2	L8
L7	l3 and (manufactur$ with tag$)	0	L7
L6	L5 and smart$	0	L6
L5	L4 and (tag$ with memor$)	5	L5
L4	L3 and (tag$ same encrypt$)	6	L4
L3	L2 and (verif$ with (product or goods) with authentic$)	46	L3
L2	L1 and (authenticat$ with (product or goods))	195	L2
L1	(authenticat$ with (product or item or part or goods)) and (crypt$ or encrypt$ or decrypt$) and @ad<=19980414	707	L1

viewed

scanned

END OF SEARCH HISTORY

9/182279

WEST

Generate Collection | Print

12/2/04 ✓

L8: Entry 1 of 2 File: USPT Jun 16, 1998

US-PAT-NO: 5768384
DOCUMENT-IDENTIFIER: US 5768384 A

TITLE: System for identifying authenticating and tracking manufactured articles

DATE-ISSUED: June 16, 1998

INVENTOR-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY
Berson; William	Weston	CT		

ASSIGNEE-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Pitney Bowes Inc.	Stamford	CT			02

APPL-NO: 08/ 623078 [PALM]
DATE FILED: March 28, 1996

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/23; 380/51, 705/11, 705/28
US-CL-CURRENT: 705/50; 235/385, 380/51, 705/11, 705/28, 713/178

FIELD-OF-SEARCH: 380/51, 380/23, 283/74, 705/11, 705/28, 705/29

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5384846	January 1995	Berson et al	
☐	5420924	May 1995	Berson et al.	
☐	5426700	June 1995	Berson	
☐	5592561	January 1997	Moore	380/51 X
☐	5666421	September 1997	Pastor et al.	380/51

ART-UNIT: 224

PRIMARY-EXAMINER: Dombroske; George M.

ASSISTANT-EXAMINER: Felber; Joseph L.

ATTY-AGENT-FIRM: Reichman; Ronald Scolnick; Melvin J. Meyer; Robert

6/4/03 2 4

ABSTRACT:

This invention relates to a system for identifying, authenticating and tracking articles of manufacture throughout their manufacturing and distribution channels. The foregoing system utilizes: manufacturing meters that are located at authorized manufacturing locations and produce encrypted data that is uniquely associated with each manufactured article; a printer located at the authorized manufacturing locations so that the printer will print the information encrypted by the meter, which encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article.

22 Claims, 3 Drawing figures

DOCUMENT-IDENTIFIER: US 5768384 A
TITLE: System for identifying authenticating and tracking manufactured articles

Abstract Text (1):
This invention relates to a system for identifying, authenticating and tracking articles of manufacture throughout their manufacturing and distribution channels. The foregoing system utilizes: manufacturing meters that are located at authorized manufacturing locations and produce encrypted data that is uniquely associated with each manufactured article; a printer located at the authorized manufacturing locations so that the printer will print the information encrypted by the meter, which encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article.

Application Filing Date (1):
19960328

Brief Summary Text (14):
This invention overcomes the disadvantages of the prior art by providing a system for identifying, authenticating and tracking articles of manufacture or manufactured goods throughout their manufacturing and distribution channels. The foregoing system utilizes: manufacturing meters that are located at authorized manufacturing locations and produce encrypted data that is uniquely associated with each manufactured article; a printer located at the authorized manufacturing locations so that the printer will print the information encrypted by the meter, which encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article.

Brief Summary Text (15):
Manufacturing meters are used to create unique encrypted labels or tags which are associated with and affixed to the manufactured article from the moment the article is manufactured. The label or tag contains a time stamp and some identification of the manufactured article. The manufactured article may be identified by the following manufacturing information: the location in which the article was manufactured; the machine that produced the article; the person who operated the machine that produced the article; and the serial number of the article, etc. The manufactured article may also be identified by having information that may be used downstream in the distribution chain. For instance, the customs rating code, and shipping manifest data. The manufacturing and distribution chain information is encrypted and/or secured with a digital signature and printed as a code on the aforementioned label or tag. The code may be encrypted and be visible or invisible to the unaided human eye. The data center is in periodic communication with the manufacturing meters and is used to distribute encryption certificates to the manufacturing meters, record the forensic integrity of the manufacturing meters and log the usage of the manufacturing meters. The scanners are used to read and determine the authenticity of the information printed on the tags or labels.

Detailed Description Text (2):

this is ONLY a specific situation

Referring now to the drawings in detail and more particularly to FIG. 1, the reference character 11 represents a sticker that is affixed to box 12. Box 12 contains articles. The type of articles contained in box 12, is 9720 Plain Paper Facsimile 13. The distributor of the articles is shown at 14, the city in which the distributor is located at 15, the type of equipment for which the articles may be used at 16, the color of the articles 17 and the lot number of the articles 18. A label 20 containing an encrypted bar code or a normal bar code 21, that is developed by some or all of the information contained on sticker 11, is affixed to sticker 11. It will be obvious to one skilled in the art that bar code 21 may be printed with an ink that is visible or invisible to the unaided human eye.

Detailed Description Text (3):
FIG. 2 is a drawing of a order form 26 that may be used to order manufactured articles. The serial number 27 of order form 26 of company 28 is dated at 29, transmitted to 30, by 31, regarding parts and supplies order request 32. The supply items# are indicated in column 33, the part numbers in column 34, the quantities ordered in column 35 and a description of the manufactured articles in column 36. The person requesting the manufactured articles is indicated at 37 and their address and telephone at 38. Information regarding the ordering of 9720 plain white facsimile paper is entered in columns 33, 34, 35 and 36. A label 9 containing an encrypted bar code or a normal bar code 8, that is developed by some or all of the information contained on order form 26, is affixed to order form 26. It will be obvious to one skilled in the art that bar code 8 may be printed with an ink that is visible or invisible to the unaided human eye. It will also be obvious to one skilled in the art that various other forms i.e., customs forms, shipping manifests, production forms, etc. may be used to replace form 26. Any of the above mentioned forms may be stored in any tangible medium of expression i.e., computer memory, diskettes, paper, etc.

Detailed Description Text (4):
FIG. 3 is a block diagram showing the interaction of manufacturing meter 25, manufacturing information input device 39, data center 40 and scanner 56 of the apparatus of this invention. The components of manufacturing meter 25 are contained in a secure box 46, that includes physical interlocks or sensors 53 that prevent unauthorized personnel from tampering with the components of meter 25. Sensors 53 communicate with data center 40 via encryptor 43. An example of box 46 is the Veritas.TM. Authenticator manufactured by Pitney Bowes of Shelton, Conn. 06484.

Detailed Description Text (5):
Manufacturing meter 25 includes: a secure clock 42, that indicates the time information was inputted by device 48 to meter 25; a encryptor 43, that is coupled to clock 42; an account meter 44 that includes an ascending register and a descending register, that are coupled to encryptor 43, a bar code generator 45, that is coupled to encryptor 43; a processor 52 that is coupled to account meter 44 and encryptor 43, and a test key 47, that is coupled to data center 40 and encryptor 43.

Detailed Description Text (6):
Manufacturing information input device 39 includes: an input device 48, that is coupled to clock 42, encryptor 43 and account meter 44 of manufacturing meter 25; a card reader 49 that is coupled to input device 48; an operators identification card 50 that is read by reader 49; and a manufactures location authorization card 51 that is read by reader 49. Card 50 may be a card that has a bar code or other code affixed thereto that contains information about the person who is operating the equipment that is producing the manufactured article. The information encoded in card 50 may be the name, social security number, age, height, weight, color of eyes, etc. of the operator of the equipment that is producing the manufactured article. Card 51 may be a card that has a bar code or other code affixed thereto that contains information about the manufacturer who owns, leases, or rents the equipment that is producing the manufactured article. The information encoded in card 51 may be the name, tax identifying number, location of the main office, etc. of the manufacturer that is producing the manufactured article. Input device 48 may be used to inform meter 25 of the serial number of the machine or machines producing the manufactured article, the location of the machine or machines producing the manufactured article; and/or a description of the components that are used to produce the manufactured article, etc.

Detailed Description Text (7):
Periodically, manufacturing meter 25 is inspected by the enabling of test key 47.

Test key 47 may be a physical key or a signal from data center 40 and/or an encrypted signal from encryptor 43.

Detailed Description Text (9):
In operation encryptor 43 and processor 52 will be programmed with an encryption algorithm, as is known in the art. Reference can be had to U.S. Pat. No. 4,853,961, 5,073,935 and 5,142,577, herein incorporated by reference wherein suitable encryption schemes are disclosed. In addition, a standard encryption scheme, such as the RSA encryption technique, can also be used for the programming of processor 52.

Detailed Description Text (10):
Bar code generator 45 will encode the information received from encryptor 43 to create a unique encrypted bar code that is associated with the article that was manufactured. Generator 45 is coupled to printer 54, which is located at the site that produced the manufactured article. Generator 45 will cause printer 54 to print a unique bar code on a product label or tag 55. The aforementioned bar code may be visible or invisible to the unaided human eye. Label or tag 55 is affixed to the manufactured article. The aforementioned bar code on tag 55 contains encrypted or digitally signed data files representing information that is unique to the article manufactured.

Detailed Description Text (11):
In order to ascertain if the article manufactured that has tag 55 affixed thereto is genuine and not diverted from its intended logistics channel, the bar code on tag 55 is scanned by scanner 56. The encrypted information contained in the bar code printed on tag 55 is retrieved and then compared against information retrieved from the scan of associated documents. For instance, scanner 56 may scan the information contained in invoice 26. It will be obvious to one skilled in the art that many different associates documents pertaining to the manufactured article may be scanned by scanner 56. If the scanned information on tag 55 matches or is correctly related to the scanned information on invoice 26 (the manufactured article is in the correct distribution channel and the article is genuine). If, for example the scanned article is genuine, but the scanned article does not belong to the articles covered by invoice 26, then the manufactured article is a forgery or diverted genuine article.

Cite

CLAIMS:

1. A system for identifying, authenticating and tracking articles of manufacture, said system comprising:

one or more manufacturing meters that are located at authorized manufacturing location, said meters produce encrypted information that is uniquely associated with each manufactured article and the operator of the equipment that produced the manufactured article;

one or more printers located at the authorized manufacturing locations wherein each of said printers is coupled to one of said manufacturing meters, that is located at the same location as said printer, so that said printers print the information encrypted by said meters, which encrypted information is affixed to the manufactured article;

means for producing information that is used to identify the manufactured article; and

means for identifying the authenticity of the manufactured articles by comparing the encrypted information printed on the article with the information produced by said producing means.

2. The system claimed in claim 1, further including:

a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters, said data center determines the number of manufactured articles in which encrypted information may be affixed.

3. The system claimed in claim 2, wherein said manufacturing meter further comprises:

an ascending register that maintains a record of the number of articles for which encrypted information has been produced; and

a descending register that maintains a record of the number of articles which encrypted information has been authorized to be printed by said data center.

5. The system claimed in claim 1, wherein the information encrypted by said meter contains a time stamp that identifies the time the manufactured article was produced.

6. The system claimed in claim 1, wherein the information encrypted by said meter includes the location in which the article was manufactured.

7. The system claimed in claim 1, wherein the information encrypted by said meter includes the machine that produced the article.

8. The system claimed in claim 1, wherein the information encrypted by said meter includes the name of the person who operated the machine that produced the article.

9. The system claimed in claim 1, wherein the information encrypted by said meter includes the serial number of the article.

13. The system claimed in claim 1, wherein said means for producing information produces encrypted information.

14. The system claimed in claim 13, wherein the encrypted information may be invisible or invisible to the unaided human eye.

16. The system claimed in claim 1, wherein the information encrypted by said meter includes the social security number of the person who operated the machine that produced the article.

17. The system claimed in claim 16, wherein the information encrypted by said meter includes the age of the person who operated the machine that produced the article.

18. The system claimed in claim 17, wherein the information encrypted by said meter includes the color of the eyes of the person who operated the machine that produced the article.

19. A method for determining if a manufactured article is the same article described in a medium of expression, comprising the steps of:

a. producing encrypted data on a manufactured article that is uniquely associated with the manufactured article and the operator of the equipment that produced the manufactured article;

b. producing information pertaining to the manufactured article on a medium of expression;

c. encrypting at least a portion of the produced information on a medium of expression;

d. placing at least a portion of the encrypted information derived in step c on the medium of expression;

e. comparing the information encrypted on the manufactured article with the information encrypted on the medium of expression;

f. determining if the information in step e compares in order to authentic the article.

20. The method of claim 19, further including the steps of:

determining the number of manufactured articles in which encrypted information may be affixed.

End of Result Set

Generate Collection | Print

L10: Entry 2 of 2 File: USPT Sep 30, 1997

DOCUMENT-IDENTIFIER: US 5673318 A
TITLE: Method and apparatus for data authentication in a data communication environment

US Patent No. (1):
5673318

CLAIMS:

1. An article of manufacture for allowing a data processing system to determine an authentication tag to be used in conjunction with transfer of data using a communication channel comprising:

a computer readable medium having computer program code embodied therein, the program code comprising:

means for partitioning said data into a plurality of blocks in a system memory;

means for encoding each of said blocks to create a word that represents both a value of each of said blocks and an identifier of each of said blocks;

means for applying a pseudo-random function to each said word to create a plurality of enciphered words;

means for combining said plurality of enciphered words to create a tag;

means for combining the tag and at least some data to create a data packet; and

means for transmitting the data packet over the communication channel.

7. An article of manufacture for allowing a data processing system to determine an authentication tag to be used in conjunction with transfer of data using a communication channel comprising:

a computer readable medium having computer program code embodied therein, the program code comprising:

means for partitioning said data into a plurality of blocks;

means for combining with each of said blocks a block identifier to create a word;

means for applying pseudo-random function to (i) each said word and (ii) an identifier for said data to create a plurality of enciphered words;

means for combining said plurality of enciphered words to create a tag;

means for combining the tag and at least some data to create a data packet; and

means for transmitting the data packet over the communication channel.

End of Result Set

Generate Collection | Print

Y ✓

L10: Entry 2 of 2 File: USPT Sep 30, 1997

US-PAT-NO: 5673318
DOCUMENT-IDENTIFIER: US 5673318 A

TITLE: Method and apparatus for data authentication in a data communication environment

DATE-ISSUED: September 30, 1997

INVENTOR-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY
Bellare; Mihir	New York	NY		
Guerin; Roch Andre	Yorktown Heights	NY		
Rogaway; Phillip Walder	Austin	TX		

ASSIGNEE-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 08/ 647503 [PALM]
DATE FILED: May 14, 1996

PARENT-CASE:
This Application is a continuation of Ser. No. 08/052,304 filed on Apr. 23, 1993, now abandoned.

INT-CL: [06] H04 L 9/00, H04 L 9/06

US-CL-ISSUED: 380/23; 380/9, 380/25, 380/29, 380/49
US-CL-CURRENT: 713/170; 380/29, 713/181

FIELD-OF-SEARCH: 380/4, 380/9, 380/23, 380/25, 380/29, 380/46, 380/49, 380/50

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5369705	November 1994	Bird et al.	380/23 X

ART-UNIT: 222

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: LaBaw; Jeffrey S.

ABSTRACT:

A method and system for providing data authentication, within a data communication environment, in a manner which is simple, fast, and provably secure. A data message to be sent is partitioned into data blocks. Each data block is combined with a block index to create a word. A pseudo-random function is applied to each word to create a plurality of enciphered data strings. An identifying header, comprising the identity of the sender and a counter value, is also enciphered using a pseudo-random function. These enciphered data strings and header are logically combined to create a tag. As the enciphering of a particular word occurs independent of the other words, each block can be enciphered independently of the others. The method and system can thus be performed and structured in either a parallel or pipelined fashion. A receiving component or system generates a second tag which can then be compared with the transmitted tag to determine message authentication.

20 Claims, 10 Drawing figures

9/192279

WEST

Generate Collection | Print

A, Y

L5: Entry 1 of 5 File: USPT Nov 15, 1988

US-PAT-NO: 4785290
DOCUMENT-IDENTIFIER: US 4785290 A

TITLE: Non-counterfeitable document system

DATE-ISSUED: November 15, 1988

INVENTOR-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY
Goldman; Robert N.	Kailua	HI		

ASSIGNEE-INFORMATION: NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Light Signatures, Inc.	Los Angeles	CA			02

DISCLAIMER DATE: 20001227

APPL-NO: 07/ 045004 [PALM]
DATE FILED: April 30, 1987

PARENT-CASE:
RELATED SUBJECT MATTER This is divisional of application Ser. No. 728,553, filed Apr. 29, 1985, now U.S. Pat. No. 4,663,622, which is in turn a divisional of application Ser. No. 623,654, filed June 22, 1984, now U.S. Pat. No. 4,546,352, which is in turn a divisional of application Ser. No. 492,324, filed June 3, 1983, now U.S. Pat. No. 4,489,318, which is in turn a divisional of application Ser. No. 276,282, filed June 22, 1981, now U.S. Pat. No. 4,423,415, which is in turn a continuation-in-part of Ser. No. 161,838 filed June 23, 1980, and entitled "Non-Counterfeitable Document System" now abandoned.

INT-CL: [04] G06K 5/00, G06F 7/04

US-CL-ISSUED: 340/825.34; 235/380
US-CL-CURRENT: 340/5.86; 235/380, 340/5.9, 380/51, 380/54, 713/168, 713/185

FIELD-OF-SEARCH: 340/825.34, 340/825.33, 235/480, 235/380, 235/487, 356/71, 283/72-74, 283/91, 283/82, 350/3, 350/61

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL

	PAT-NO	ISSUE-DATE	PATENTEE-NA	US-CL
☐	3412493	November 1968	French	40/2.2
☐	4006050	February 1977	Hurst et al.	156/234
☐	4014602	March 1977	Ruell	350/3.61
☐	4034211	July 1977	Horst et al.	356/71
☐	4527051	July 1985	Stenzel	235/380
☐	4591707	May 1986	Stenzel et al.	235/493
☐	4663622	May 1987	Goldman	340/825.34

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
529398	November 1972	CH	340/825.34
569333	November 1975	CH	340/825.34

ART-UNIT: 264

PRIMARY-EXAMINER: Yusko; Donald J.

ATTY-AGENT-FIRM: Nilsson, Robbins, Dalgarn, Berliner, Carson & Wurst

ABSTRACT:

A system is disclosed for authenticating an object on the basis of certain physical phenomena or character, specifically, measurable, but not practicably duplicable random variations in the object. In one form, the object (authenticator (T)) is a paper tag having a reference space (14), the varying translucency pattern of which is a measurable but practicably unduplicable characteristic of the paper. The reference space (14) is sensed to provide reference signals indicative of the varying translucency. A reference numeral (10) is then provided from some registered form, as on the tag or in a list. If the numeral (10) is readily accessible, it likely will be cryptographically encoded. Note the value of putting encoded information on the tag to avoid the need for large reference files. For verification, freshly sensed reference signals, as from the tag (T) (actually characteristic of the tag) are compared with signals that previously were sensed as characteristic of the tag (T). Structures are disclosed as specific forms of the authenticator (T), along with apparatus for authenticator production, detection and manipulation. Different forms of tags (210) are disclosed, the measurable characteristic of which involves light transmissivity and reflectivity. Apparatus (111) for spectrographic confirmation of tag material is also disclosed. In an illustrative form of a tag (T) as an identification means, tags and processing apparatus utilize magnetic medium (218) and printed images (214). The magnetic medium is also disclosed to be recorded as for developing information on shelf life and sales channels.

20 Claims, 19 Drawing figures

L5: Entry 1 of 5 File: USPT Nov 15, 1988

DOCUMENT-IDENTIFIER: US 4785290 A
TITLE: Non-counterfeitable document system

Abstract Text (1):
A system is disclosed for authenticating an object on the basis of certain physical phenomena or character, specifically, measurable, but not practicably duplicable random variations in the object. In one form, the object (authenticator (T)) is a paper tag having a reference space (14), the varying translucency pattern of which is a measurable but practicably unduplicable characteristic of the paper. The reference space (14) is sensed to provide reference signals indicative of the varying translucency. A reference numeral (10) is then provided from some registered form, as on the tag or in a list. If the numeral (10) is readily accessible, it likely will be cryptographically encoded. Note the value of putting encoded information on the tag to avoid the need for large reference files. For verification, freshly sensed reference signals, as from the tag (T) (actually characteristic of the tag) are compared with signals that previously were sensed as characteristic of the tag (T). Structures are disclosed as specific forms of the authenticator (T), along with apparatus for authenticator production, detection and manipulation. Different forms of tags (210) are disclosed, the measurable characteristic of which involves light transmissivity and reflectivity. Apparatus (111) for spectrographic confirmation of tag material is also disclosed. In an illustrative form of a tag (T) as an identification means, tags and processing apparatus utilize magnetic medium (218) and printed images (214). The magnetic medium is also disclosed to be recorded as for developing information on shelf life and sales channels.

Application Filing Date (1):
19870430

Brief Summary Text (4):
Individual serial numbers or other identifications have also been applied to products for the purpose of authentication. Yet, failing either complete cooperation from sales people, or a comprehensive detection and policing program, such techniques afford little protection against copies. As a result of such difficulties, product pirates have been relatively free to pick and choose from a current group of successful products that could be copied, the fakes to be sold on a global scale with relative impunity.

Brief Summary Text (5):
In addition to commercial products, authentication is important in a variety of other applications as for commercial paper, identification cards, documents of value, and so on. As disclosed herein, the system of the present invention may be variously implemented to authenticate a wide range of subjects, including people.

Brief Summary Text (6):
The present invention is based on recognizing that an effective system of authentication can utilize a device with an obscure random characteristic. The system also recognizes that objects with such characteristics are readily available so that authentication devices hereof can be produced and used inexpensively, enabling selective investigation. For example, a producer can provide his fullline of products with an authenticator, then limit policing activities to either sample groups or those select, very successful products that are most likely to be copied.

Brief Summary Text (11):
In one exemplary application, reference signals identifying a pattern and its

location are cryptographically encoded and recorded on the medium to provide a self-contained tag. Pursuing such an example in more detail, assume that the physical medium of the authenticators comprises bond paper. A defined area of each sheet of paper has a specified pattern of selected locations. Based on the characteristic of that pattern (and its location), reference signals are generated to be encoded and associated with the sheet, e.g. printed or otherwise recorded, as on the sheet. To authenticate such a sheet, the system of the present invention senses it to again detect or measure the selected pattern of authentication signals. The fresh signals are then compared to the recorded reference signals previously developed from the pattern. Coincidence of the signals indicates the sheet to be genuine.

Brief Summary Text (12):
As disclosed in detail below, the system hereof may be variously implemented using different media and techniques. For example, the location of the random pattern of concern may be visually obscure and can be crytographically encoded by a computer apparatus. Also, the characteristic reference signals can be variously stored for future comparisons. Some or all of such signals might be kept on a list, or cryptographically encoded and recorded, in memory, or optically or magnetically on the authenticator media.

Drawing Description Text (3):
FIG. 1 is a perspective view of an authenticator tag according to the present invention illustrated for use in association with a product;

Detailed Description Text (3):
Referring initially to FIG. 1, a shoe S is fragmentarily represented along with an authenticator tag T which is securely attached to the shoe by a cord C. The tag T carries a legend in the form of a reference number 10 which may be duplicated in the shoe, e.g. number 12. In general, the system of the present invention enables authentication of the tag T to verify that the shoe S is a genuine article. First, the tag T is identified with the shoe S by the similar numbers and 12. However, more significantly, the number 10 indicates and specifies a measurable but not practicably duplicable physical characteristic of the tag T. Specifically, in a space 14 (generally designated on the tag T) a field of locations (array of squares) is defined (not actually marked in detail) which has a characteristic measurable, but not practicably duplicable pattern of variations in translucency. The location of that pattern and its form are defined by a representative number that is cryptographically related to the identical numbers 10 and 12. That is, a pattern of locations in the space 14 and their translucency are coded into the reference number 10.

Detailed Description Text (4):
It is to be realized that the tag T (if authentic) verifies the genuine nature of the particular shoe S only because the identification numbers 10 and 12 coincide. For an alternative more direct authentication, the medium of the space 14 may be integrated in the actual product that is to be identified, or other codes can be employed. For example, in the case of art work, e.g., signed graphic prints, a marginal area of the sheet of paper bearing the print may serve to provide the pattern of measurable but not duplicable random variations. For other products, other characteristics can be utilized. However, note that a specific tag T may be employed only to identify a single article. That is, while the tag T might be affixed to a fake duplicate of the shoe S, such a switch to the counterfeit shoe would leave the genuine shoe S without an authenticator thereby presumably reducing its value.

Detailed Description Text (5):
In alternative implementations, the tag T might be completely blank or could carry only an indication of the coded locations. In such implementations, the pattern locations could be uniform and the information on the characteristic pattern could be kept on an inventory or list of specific products or objects. Comparing a freshly sensed characteristic pattern with the recorded characteristic pattern would then authenticate a product. Such implementations could be desirable for items of limited production or large monetary value, e.g., graphic art prints.

Detailed Description Text (17):
The reference number 10 (FIG. 1) in a format in accordance with the above table is used in a signal represented form, identified as a code word PN. It is to be appreciated that the first sixteen digits (decoded word DW including words SD, AN,

and CC above) are cryptographically coded into a code word designated CW. Consequently, the code word CW may not identify directly with the digits of the decoded word DW, although the data of each include: one digit indicative of the offset or location of the array 28, nine digits which indicate the six predetermined locations or addresses of the selected squares in the array pattern, and six digits indicative of the translucency at the selected squares.

Detailed Description Text (20):
The word PN is completed with miscellaneous data as indicated above and reduced to the form of the reference number 10 which is printed on the authenticator tag T. The tag T is then available for authentication to verify the likelihood that an associated product is genuine without reference to other memory. Thus, it is not necessary in this implementation to store inventories of tag characteristic data separate from the tags themselves.

Detailed Description Text (21):
In the authentication or test operation, the authentication system of this embodiment cryptographically decodes a portion of number 10 (code word CW) to provide the decoded word DW. That word indicates: the precise location of the observed pattern of squares 29 in the array 28 (FIG. 5) and the digits indicative of the previously observed value of the physical characteristic at each of such individual squares.

Detailed Description Text (34):
A variety of cryptographic encoders are well known in the prior art and may be employed in embodiments of the present invention. As illustrated in FIG. 7, a form of cryptographic encoder 58 receives the contents of the register 56 (sixteen digits of the word DW) for cryptographic encoding to provide the coded word CW for the printed reference number 10. The digits of the word CW are supplied to a register 60 which also receives the miscellaneous data portion or code word IW from a register 62. In that fashion, the register 60 receives the reference number PN which, in one operating format, is imprinted on the tag T (FIG. 1).

Detailed Description Text (35):
The register 60 may incorporate a readout device for providing the reference number 10 (representative of word PN). Alternatively, the signals representative of the number may be employed to drive any of a variety of printing mechanisms to imprint the identification number on the tag authenticators T. If desired, as indicated above, the identification number may also be placed on the article or product for sale (number 12, FIG. 1). In an another arrangement, the PN register 60 may be connected to a magnetic recorder 64 for recording the number PN on the authenticator it identifies, the authenticator incorporating a magnetic recording surface as disclosed in detail below. A system of continuous operation for producing complete authenticators also is described below.

Detailed Description Text (38):
Signal representations from the register 72 (comprising the code word CW) are applied to a cryptographic decoder 74 which functions during an interval of a timing signal tb to develop the decoded word DW, signal representations for which are placed in a register 76 during the interval of the timing signal tc.

Detailed Description Text (41):
The comparator 78 provides signals to indicate the degree of coincidence between those two code words. Specifically, the comparator 78 supplies a signal to a display apparatus 80 which may indicate any one of the numerals: "0","1", "2", and "3". Exhibition of the numeral "0" indicates no significant degree of comparison thereby designating the tag T as a fraud. Display of the numeral "1" indicates a small degree of coincidence, e.g. two of the six digits may compare. In a related fashion, the display of numeral "2" indicates a greater degree of comparison, and the numeral "3" indicates full coincidence. Thus, the observer is afforded with an indication of the degree of coincidence; and in that regard, some latitude may be tolerable or desirable as part of an acceptable authentication. As indicated above, the display 80 may also manifest various data as the product batch number or even a specific product number. In that manner, the system of the present invention is useful in detecting diversion of products as well as the counterfeiting of products.

Detailed Description Text (42):
From the above description, it may be seen that the system of the present invention affords an authenticator that cannot be production copied in a commercially

practical device. The cryptographic code may range from being a relatively simple one, requiring only manual decoding, to a complex code requiring computer decoding with a randomly generated computer key stored in the computer, and unknown to any living person.

Detailed Description Text (43):
Considering various degrees of comparison which may be sensed as disclosed in the system of FIG. 8, the material of the authenticator and its environment may permit use to a standard of complete coincidence. However, with regard to other products, considerable tolerance may be advisable to allow for damage to a portion of the authenticator. In that regard, tests on various fibrous materials including paper tag or label stock indicate a wide variety of media that meet the requirement of being repeatably scannable, preservable, and unique with regard to the translucency patterns discussed above.

Detailed Description Text (51):
One portion of the word PN, i.e. the cryptographically encoded word CW, comprises the first sixteen digits of the word PN. The remaining portion of the word PN (word IW consisting of ten digits) is not cryptographically encoded and simply indicates miscellaneous information or data, e.g. the date of encoding, an identification of the cryptographic encoding technique used, product information, and the like. Signals representative of the code word IW are supplied from the register 126 to a display unit 128 for direct display illustrated as "data" in FIG. 8.

Detailed Description Text (52):
The cryptographically encoded word CW is supplied from the register 126 to a cryptographic decoder 130. As a result, the sixteen coded digits are decoded to provide the code word DW which is then set in a register 132 (center right). The word DW consists of three parts, specifically: (1) the digit SD indicating the shift or offset of the array 28 from the corner indicia 16 (FIG. 1); (2) the address information word AN for locating the predetermined squares; and (3) the translucency data word CC for the translucency of the preselected squares.

Detailed Description Text (67):
That portion of the word PN which is carried in the sixteen digits designated as word CW is processed by the cryptographic decoder 130 to produce the decoded word DW which is set in the register 132. A portion of that word, i.e. the digit SD, indicates the offset of line 30 (FIG. 5) and is applied through a digital decoder 133 to the transport and pulse generator 104. Essentially, the single decimal digit SD manifests the predetermined amount of offset. Accordingly, the digit SD is decoded and used by the transport and pulse generator 104 to advance the authenticator 102 a small distance, proportional to the numerical value of the digit SD.

Detailed Description Text (75):
In an alternative implementation, deemed suitable for small production articles, the characteristic codes of authenticators may be registered in computer memory for test verification. Specifically, an authenticator (paper for example) could be measured or sensed to provide a characteristic code word for a product. The code word would then be placed on a list to be scanned for verifying an authenticator accompanying the product. Various other implementations will be apparent, including forms where part or all of the code word is carried with the product and can be obscured as disclosed in detail above, by cryptographic encoding. The pattern of predetermined squares may also be preserved in secrecy as disclosed in the above detailed embodiment. Of course, various forms of energy, record medium and so on may be employed in the system. In addition to paper, certain forms of card stock also have been found to be appropriate as being repeatably scannable, preservable and unique. As suggested above, spectral response variations may also be used for further assurance against counterfeits.

Detailed Description Text (132):
As each of the perforations separating a pair of tags 328 move under the head 334, the anomaly is sensed indicating that a fresh tag 328 is about to move between the sensors 338 and the lamp 336. As such movement occurs, analog translucency signals are provided to the computer in a time-space relationship with the tag 328 being observed. Such signals are processed by the computer, specifically being sampled at select locations, and the samples converted to a digital form. Signals definitive of the sampled locations are also developed in digital form. Accordingly, the digital signals indicate specific locations on the tag 328 under consideration and the

translucency at such locations. A representative code word (encrypted) is then formed for recordation on the stripe 330 of the tab [redacted].

Detailed Description Text (137):
Generally, the authenticator is used by selecting a path in relation to certain of the engraved dots, e.g., a path 360 between the dots 354 and 359. The measurable but not practicably duplicable characteristic is then sensed along the path 360 to provide a signal that identifies the paper 350. The path 360, as well as the observed analog signal may be registered in an encrypted numeral 362. Accordingly, authentication of the paper 350 involves decoding the numeral 362, sensing the measurable but not practicably duplicable characteristic along the path 360, then comparing (at least in part) the sensed characteristic with the values registered for that characteristic.